Aula 05

GRUPOS QUOCIENTES

METAS

Estabelecer o conceito de grupo quociente.

OBJETIVOS

Definir classes laterais e estabelecer o teorema de Lagrange.

Aplicar o teorema de Lagrange na resolução de problemas.

Reconhecer subgrupos normais e aplicar suas propriedades.

Reconhecer e exemplificar grupo quociente.

PRÉ-REQUISITOS

O curso de Fundamentos de Matemática e os conteúdos estudados nas aulas anteriores.

INTRODUÇÃO

Ola! Estamos em mais uma das nossas aulas. Na aula passada tivemos o nosso primeiro contato com a teoria dos grupos estudando as primeiras definições e contemplando vários exemplos. Nesta aula continuaremos a estudar os grupos onde estabeleceremos os conceitos de classes laterais, subgrupos normais e o conceito de grupo quociente que é uma das noções básicas mais importantes da álgebra abstrata.

CLASSES LATERAIS E O TEOREMA DE LAGRANGE

Sejam G um grupo, H um subgrupo e $a \in G$. Os subconjuntos de G, $aH = \{ah;\ h \in H\}$ e $Ha = \{ha; h \in G\}$ são chamados classe lateral à esquerda e classe lateral à direita de H, respectivamente.

Exemplo 1. Vamos considerar $G = S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ onde

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

que tem a seguinte tabela de operação, na qual o produto tem como 1º fator o elemento da coluna.

$\cdot$	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_4	σ_5	σ_2	σ_3
σ_2	σ_2	σ_3	e	σ_1	σ_5	σ_4
σ_3	σ_3	σ_2	σ_5	σ_4	e	σ_1
σ_4	σ_4	σ_5	σ_1	e	σ_3	σ_2
σ_5	σ_5	σ_4	σ_3	σ_2	σ_1	e

Para $H = <\sigma_4> = \{e, \sigma_3, \sigma_4\} = \{\sigma_4^m; m \in \mathbb{Z}\}$, $H\sigma_1 = \{e.\sigma_1, \sigma_3.\sigma_1, \sigma_4.\sigma_1\} = \{\sigma_1, \sigma_2, \sigma_5\}$ e $\sigma_1 H = \{\sigma_1.e, \sigma_1.\sigma_3, \sigma_1.\sigma_4\} = \{\sigma_1, \sigma_5, \sigma_2\}$.

Observação. Neste nosso exemplo, ocorreu que $H\sigma_1 = \sigma_1 H$. Em geral $H\sigma_1 \neq \sigma_1 H.$

Vamos agora estabelecer uma relação de equivalência num grupo G, na presença de um subgrupo H, onde o conjunto quociente módulo esta relação é exatamente o conjunto das classes laterais à direita, de H.

Definição 1. Seja G grupo $H \leq G$. Para cada par a, b de elementos de G, dizemos que a é congruente a b módulo H, e escrevemos $a \equiv b(modH)$ se $ab^{-1} \in H$.

Ou melhor: $a, b \in G. \quad a \equiv b(modH) \Leftrightarrow ab^{-1} \in H.$

Proposição 1. A relação binária definida no grupo G, acima é de equivalência.

Demonstração: Como $e = a.a^{-1} \in H, \forall a \in G$, seque que esta relação é reflexiva. Se $a \equiv b(modH)$ estão $ab^{-1} \in H$ e como H é um grupo, $ba^{-1} = (ab^{-1})^{-1} \in H$ donde temos $b \equiv a(modH)$ e, a relação é simétrica.

Finalmente, se $a, b, c \in G$ são tais que $a \equiv b(modH)$ e $b \equiv c(modH)$, então $ab^{-1}, bc^{-1} \in H$. Novamente, do fato de que H é grupo temos $ab^{-1}, bc^{-1} \in H$, isto é, $ac^{-1} \in H$, ou seja, $a \equiv c(modH)$ e, portanto, a relação é transitiva.

Como sabemos a classe de equivalência do elemento $a \in G$ é por definição.

$\bar{a} = \{x \in G; x \equiv a(modH)\}$.

Notemos que $x \equiv a(modH) \Leftrightarrow x\mathrm{a}^{-1} \in H \Rightarrow \exists h \in H$ tal que $xa^{-1} = h \Leftrightarrow x = ha \Rightarrow x \in Ha$. Logo, $\bar{a} \subset Ha$. Se $x \in Ha$ então $\exists h \in H$ tal que $x = ha$ e neste caso $h = xa^{-1} \in H$ implicando que $x \equiv a(modH)$, ou melhor, que $x \in \bar{a}$. Portanto $\bar{a} = Ha$.

Denotamos o conjunto quociente módulo esta relação por G/H e, escrevemos

$$\frac{G}{H} = \{Ha; a \in G\}$$

Observação. Quando G é um grupo finito obviamente o conjunto $\frac{G}{H}$ é finito e tem cardinalidade menor ou igual à ordem de G. Quando G é infinito, podemos ter $\frac{G}{H}$ finito ou $\frac{G}{H}$ infinito.

Exemplo 2. Se $G = \mathbb{Z}$ nunido da adição os subgrupos de G são os conjunto do tipo $H = n\mathbb{Z} = \{nx; x \in \mathbb{Z}\}$.

Notemos que dados $a, b \in G$, então $\equiv (\ \mathbb{Z}) \Leftrightarrow\ -\ \in \mathbb{Z} \Leftrightarrow |-$ e que $\equiv ()$. Segue que $\frac{}{\mathbb{Z}} = \{\mathbb{Z} + ;\ \in \mathbb{Z}\} = \mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{-1}\}$ para $\mathbb{Z} \neq \{0\}$. Se $n\mathbb{Z} = \{0\}$, temos $n\mathbb{Z} + a = \{a\}$ e $\frac{G}{n\mathbb{Z}} = \{\{a\}; a \in G\}$. Logo, para $n \neq 0$, $\frac{G}{n\mathbb{Z}}$ é finito e tem n elementos, enquanto que, para $\mathrm{n} = 0, isto\ \text{é}, \mathrm{H} = \{0\}, \frac{\mathrm{G}}{\mathrm{H}}$ tem infinitos elementos.

Definição 2. Dados G e $H \leq G$, definimos o índice de $H\ em\ G$ como sendo a cardinalidade do conjunto quociente ${}^{G}/_{H}$ e indicamos por $[G : H]$.

Proposição 2. (Teorema de Lagrange). Se G é um grupo finito e H é um subgrupo de G então, a ordem de H divide a ordem de G.

Demonstração: Para cada $a \in G$, a aplicação $\psi_a : H \longrightarrow Ha$ definida por $\psi_a(h) = ha$ é bijetiva. De fato, se $h_1, h_2 \in H$ e $\psi_a(h_1) = \psi_a(h_2)$ temos $h_1 a = h_2 a \Longrightarrow h_1 = h_2$. Se $b \in Ha$ então existe $h \in H$ tal que $b = ha$ e $\phi_a(h) = b$

Escrevendo $\frac{G}{H} = \{Ha_1, \dots, Ha_n\}$ onde $n = [G : H]$, como $|Ha_1| = \cdots = |Ha_n| = |H|$ e $G = \bigcup_{i=1}^{n} Ha_i$, temos que $n.|H| = |G|$. Portanto $|H|\,|\,|G|$,como queríamos demonstrar.

Exemplo 3. Como conseqüência imediata do teorema de Lagrange, todos os grupos finitos cuja ordem é um número primo são cíclicos ($\Longrightarrow$ abelianos). Com efeito, se $|G| = p$ e $a \in G \setminus \{e\}$, então $| < a > |\,|p$ e $|a| > 1 \Longrightarrow | < a > | = p \Longrightarrow < a >= G$.

SUBGRUPOS NORMAIS E GRUPOS QUOCIENTES

Definição 1. Sejam G um grupo e H subgrupo de G. Dizemos que H é um subgrupo normal de G se, para todo $h \in$ H e todo $a \in G$ temos $a^{-1}ha \in H$. Indicamos $H \trianglelefteq G$.

Exemplo 1. Quando G é abeliano, todo subgrupo H de G é normal. Com efeito, para $h \in H$ e $a \in G$, temos $a^{-1}ha = ha^{-1}a = h \in H$. Para todo G, $\mathbb{Z}(G)$ é normal. Se $b \in \mathbb{Z}(G)$ e $a \in G$, $a^{-1}ba = ba^{-1}a = b \in \mathbb{Z}(G)$.

Proposição 1. Sejam G grupo e $H \leq G$. As seguintes afirmações são equivalentes:

i) $H \trianglelefteq G$.

ii) $\forall a \in G, a^{-1}Ha = \{a^{-1}La; h \in H\} = H$.

iii) $\forall a \in G,\ Ha = aH$.

iv) $\forall a, b \in G,\ Ha.Hb = \{x.y; x \in Ha$ e $y \in Hb\} = Hab$.

v)Se $a, b, a', b' \in G,\ a \equiv a'(modH)\ e\ b \equiv b'(modH)$ então $ab \equiv a'b'(modH)$.

Demonstração. i⇒ii). Da definição de subgrupo normal, $\forall a \in G$ e $\forall h \in H,\ a^{-1}ha \in H \Longrightarrow a^{-1}Ha \subset H$. Como a é arbitrário no grupo G, trocando a por a^{-1}, vale $aHa^{-1} \subset H$. Observemos também que $aHa^{-1} \subset H \Longrightarrow a^{-1}(aHa^{-1})a \subset a^{-1}Ha \Longrightarrow H \subset a^{-1}Ha$. Portanto, vale a igualdade $a^{-1}Ha = H$, para cada $a \in G$.

ii⇒iii). Como $a^{-1}Ha = H, \forall a\ \in G$, é imediato que $a(a^{-1}Ha) = aH$, donde temos $Ha = aH$, $\forall a \in G$.

iii⇒iv). $Ha.Hb = H(aHb) = H\big((aH)b\big) = H\big((Ha)b\big) = H.(Hab) = Hab$.

iv⇒v). Como $\mathrm{a} \equiv \mathrm{a}'(\mathrm{modH})$ e $b \equiv b'(modH)$ temos que $h_1 = a'a^{-1}, h_2 = b'b^{-1} \in H$. Logo, $a' = h_1 a \in Ha$ e $b' = h_2 b \in Hb$ e daqui, $a'b' \in HaHb = Hab$. Ou seja, $\exists h \in H$ tal que $a'b' = hab \Longrightarrow (a'b')(ab)^{-1} = h \in H \Longrightarrow a'b' \equiv ab(modH)$. Portanto, $ab \equiv a'b'(modH)$.

v⇒i). Sendo $a \in G$ e $h \leftarrow H$, vamos provar que $a^{-1}ha \in H$. Para isto, seja $a' = ha$, donde $a' \equiv a(modH)$. Como $a^{-1} \equiv a^{-1}(modH)$, temos $a^{-1}a' \equiv e(modH) \Longrightarrow a^{-1}a' \in H \Longrightarrow a^{-1}ha \in H$, conseqüentemente, $H\underline{\Delta}G$.

Considerando o conteúdo da proposição acima, podemos, bem definir, a seguinte operação em ${}^{\mathrm{G}}/_{\mathrm{H}}$:

$${}^{\mathrm{G}}/_{\mathrm{H}} \times {}^{\mathrm{G}}/_{\mathrm{H}} \longrightarrow {}^{\mathrm{G}}/_{\mathrm{H}}$$

$(Ha_1, Ha_2) \rightsquigarrow Ha_1.Ha_2$ onde $Ha_1.Ha_2 = Ha_1a_2$.

Proposição 2. ${}^{\mathrm{G}}/_{\mathrm{H}}$ munido da operação, acima definida, tem estrutura de grupo.

Dados $Ha_1, Ha_2, Ha_3 \in {}^{G}/_{H}, (Ha_1.Ha_2).(Ha_3) = (Ha_1a_2).Ha_3 = H(a_1a_2)a_3 = Ha_1(a_2a_3) = Ha_1.(Ha_2a_3) = Ha_1(Ha_2.Ha_3)$.Ou seja, esta operação é associativa.

Para cada classe lateral $Ha \in {}^{G}/_{H}$, existe $H = He$ tal que

$Ha.He = Hae = Ha$ e $He.Ha = Hea = Ha$. (H é o elemento identidade).

Finalmente, para cada $Ha \in {}^{G}/_{H}$, existe Ha^{-1} tal que $Ha.Ha^{-1} = Ha^{-1}.Ha = H$ ou seja $(Ha)^{-1} = Ha^{-1}$. (existência do oposto).

Definição 2. O grupo ${}^{\mathrm{G}}/_{\mathrm{H}}$ é chamado o grupo quociente módulo H.

Lembremos que, para a operação em $\frac{\mathrm{G}}{\mathrm{H}}$ que associa ao par (Ha_1, Hb) a classe Hab, ser bem definida é necessário que $H \trianglelefteq G$. Portanto só podemos falar no grupo quociente de G por H se H for um subgrupo normal.

Proposição 3. Sejam G um grupo e $N \trianglelefteq G$.

i) Se G é abeliano então $\frac{\mathrm{G}}{\mathrm{H}}$ é abeliano.

ii) Se G é cíclico então $\frac{\mathrm{G}}{\mathrm{N}}$ é cíclico.

Demonstração. i) $Ha, Hb \in {}^{G}/_{H}$, então $Ha.Hb = Hab = Hba + Hb.Ha$.

ii) Seja $G =< a >= \{a^m; m \in \mathbb{Z}\} \Longrightarrow \frac{G}{H} = \{Ha^m; m \in \mathbb{Z}\} = \{(Ha)^m; m \in \mathbb{Z}\} =< Ha >$.

Exemplo 2. Sejam $G = S_3$ e $H = \{e, \sigma_3\sigma_4\}$. Note que $H \leq G$. Pois, a tabela

$\cdot$	e	σ_3	σ_4
e	e	σ_3	σ_4
σ_3	σ_3	σ_4	e
σ_4	σ_4	e	σ_3

Deixa claro que $H \neq \phi$ e se $\sigma, \tau \in H$ então $\sigma . \tau^{-1} \in H$.

Como $|G| = 6$ e $|H| = 3$ segue que $[G : H] = \frac{6}{3} = 2$.

Notemos que $\frac{G}{H} = \{H, H\sigma_1\}$ onde $H\sigma_1 = \{\sigma_1, \sigma_2, \sigma_5\}$.

Exemplo 3. Sejam $G = S_3$ e $N = \{e, \sigma_3, \sigma_4\}$ onde $\frac{G}{N} = \{N, N\sigma_1\}$,

Fazendo as contas, podemos verificar que $N\sigma = \sigma N, \forall \sigma \in S_6$, portanto $N \trianglelefteq G$ e $\frac{\mathrm{G}}{\mathrm{N}}$ é o grupo quociente com tabela de operações.

$\cdot$	N	$N\sigma_1$
N	N	$N\sigma_1$
$N\sigma_1$	$N\sigma_1$	N

$$N\sigma_1 . N\sigma_1 = Ne$$

RESUMO

Nesta aula, estudamos o conceito de classe lateral onde estabelecemos o teorema de Lagrange. Estudamos os conceitos de subgrupos normais e grupos quocientes e, suas propriedades.

ATIVIDADES

1. Se G é um grupo finito com 12 elementos, um subgrupo H de G pode ter 9 elementos? Justifique sua resposta.

2. Sejam G um grupo e $a \in G$. Definimos a ordem do elemento a, e indicamos por $\mathcal{O}(a)$, a ordem do subgrupo cíclico de G gerado por a. Prove que:

i) Se $a^m = e$ então $\mathcal{O}(a)|m$.

ii) Se $a, b \in G$ então $\mathcal{O}(b^{-1}ab) = \mathcal{O}(a)$.

3. Dizemos que um grupo $G \neq \{e\}$ é simples se os únicos subgrupos normais de G são $\{e\}$ e G. Dê exemplo de grupo simples.

4. Sejam G um grupo e $H \leq G$. Para cada $a \in G$, defina $H^a = a^{-1}Ha = \{a^{-1}ha; h \in H\}$. Prove que:

a) $H^a \leq G$ b) Se H é finito, $|H^a| = |H|$ c) $H \underline{\Delta} G \Leftrightarrow H^a \subseteq H, \forall a \in G$. (o subgrupo H^a é chamado um conjugado de H em G).

5. Seja $G = \{1, i, -1, -i\}$ e $H = \{1, -1\}$. Determine $G/_H$.

COMENTÁRIO DAS ATIVIDADES

Caro aluno, você deve ter notado que a resposta da pergunta da atividade 1 é justificada facilmente pelo teorema de Lagrange.

Na segunda, escrevendo a potência de base $b^{-1}ab$ e expoente igual à ordem de a explicitamente, você deve ter notado a conclusão da atividade.

Na terceira atividade, você num primeiro momento, deve ter pensado em grupos cuja ordem é um número primo.

No item a) da quarta atividade, você deve ter notado que $e \in H^a$ e que dados $a, b \in H^a$, $ab^{-1} \in H$.

No item b), você deve ter notado que á correspondência $h \longrightarrow a^{-1}ha$ é uma bijeção de H em H^a.

No item c), olhe para a correspondência do item anterior e lembre que ela vale $\forall a \in G$.

Para a quinta atividade, você deve ter imitado algum dos exemplos do texto.

Mais uma vez, lembre-se de ler o conteúdo da aula com cuidado e sempre que precisar procure os tutores.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).